No. 15-3690

IN THE UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT

DANIEL B. STORM, *et al.*,

Appellants

v.

PAYTIME, INC.,

Appellee

On Appeal from the United States District Court
for the Middle District of Pennsylvania
Case No. 14-cv-1138
The Hon. John E. Jones III

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLANTS

Marc Rotenberg
Counsel of Record
Alan Butler
Claire Gartland
Aimee Thomson
Electronic Privacy Information Center
1718 Connecticut Ave. N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140

April 18, 2016

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and 29(c), *amicus curiae* Electronic Privacy Information Center ("EPIC") certifies that it is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

Def. Sci. Bd. Task Force on Comput. Sec., *Security Controls for Computer Systems* (1970) 22
Dell SecureWorks, *Underground Hacker Markets* (2016) 13
eBay, *eBay Inc. to Ask eBay Users to Change Passwords* (May 21, 2014) 9
EPIC, *Social Security Numbers* (2016) 14
Erika Harrell, Ph.D., Bureau of Justice Statistics, NCJ 248991, *Victims of Identity Theft, 2014* (Sept. 2015) 5, 6, 15
Ernie Hayden, *Data Breach Protection Requires New Barriers*, SearchSecurity (May 2013) 23
Excellus, *Notice Of Cyberattack Affecting Excellus Bluecross Blueshield* (2015) 6
FTC, *Consumer Sentinel Network Data Book* (Feb. 2016) 6
FTC, *Guide for Assisting Identity Theft Victims* (Sept. 2013) 18, 19, 20
Guido Calabresi, *The Costs Of Accidents: A Legal And Economic Analysis* (1970) 25, 26
Harold Demsetz, *When Does the Rule of Liability Matter?*, 1 J. Legal. Stud. 13 (1972) 26
Home Depot, *The Home Depot Reports Findings in Payment Data Breach Investigation* (Nov. 6, 2014) 9
IBM, *Winning the Battle of the Breach* (2015) 22, 24
Identity Theft Res. Ctr., *2015 Data Breaches* 5
Identity Theft Res. Ctr., *2016 Data Breach Stats* (Apr. 12, 2016) 4, 5
Identity Theft Res. Ctr., *Data Breach Reports* (Dec. 31, 2014) 5, 9
Identity Theft Res. Ctr., *Data Breach Reports* (Dec. 31, 2015) 5, 6, 7, 8
Identity Theft Res. Ctr., *Identity Theft: The Aftermath* (2014) 13
Identity Theft Res. Ctr., *ITRC Breach Statistics 2005 – 2015* (2016) 4
Identity Theft Res. Ctr., *The Limits of ID-Theft Protection and Credit Monitoring* (Aug. 10, 2015) 19
Jessica Silver-Greenberg, Matthew Goldstein, & Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. Times (Oct. 2, 2014) 9
Kim Zetter, *Four Indicted in Massive JP Morgan Chase Hack*, Wired (Nov. 10, 2015) 9
Kroll, *Data Breach Prevention Tips* (2015) 22, 23, 24
Laura Shin, *Why Medical Identity Theft Is Rising and How to Protect Yourself*, Forbes (May 29, 2015) 18
Lillian Ablon, Martin C. Libicki, & Andrea A. Golayix, RAND Corp., *Markets for Cybercrime Tools and Stolen Data* (2014) 12
Maggie McGrath, *Target Data Breach Spilled Info On As Many As 70 Million Customers*, Forbes (Jan. 10, 2014) 10

INTEREST OF THE AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.[1] EPIC routinely participates as *amicus curiae* before federal and state courts in cases concerning consumer privacy rights. *See* Mot. for Leave to File Amicus Br.

SUMMARY OF THE ARGUMENT

America faces an epidemic of data breaches that has exposed millions of consumers to identity theft and financial fraud. Criminals trade in stolen Social Security Numbers ("SSNs"), credit card numbers, and personal information. In the face of this national threat, the Court should not deny individuals the right to seek remedies for the failure of companies to protect their sensitive personal information. Raising standing barriers to legitimate claims will only allow the continued escalation of identity theft in the United States.

When the Court addressed this issue five years ago in *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), the problem of identity theft was not well understood and the information on data breach not readily available. Since that time, the problems of identity theft and data breach have become a central concern of lawmakers and courts across the country. Courts have now recognized that

[1] In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief. This brief was not authored, in whole or in part, by counsel for a party.

individuals whose personal information was stolen need not prove damages before they get through the courthouse door. *See Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693–94 (7th Cir. 2015).

Given the understanding today of the scope of the problem, this Court should hold that a data breach is an "injury-in-fact" that gives rise to Article III standing. For the purposes of establishing standing, courts should not require that the downstream consequences—untangling a stolen identity, recovering unauthorized payments, or repairing damaged credit—have already occurred before a plaintiff can bring suit. The plaintiff may need to establish harm to recover damages, but that issue is separate from consideration of standing and Article III jurisdiction.

If the Court does not permit individuals whose personal information has been mishandled and obtained by criminals to pursue redress, the problems of data breach and identity theft will only get worse. Many data breaches are avoidable; companies that collect and store sensitive information are in the best position to take the reasonable measures necessary to protect the data. Shielding these companies, *who have chosen to collect and use personal information*, from liability will remove the incentives to adopt necessary data security measures.

ARGUMENT

The lower court in this case has misconstrued the Supreme Court's standing doctrine in order to deny plaintiffs the opportunity to seek remedies for a data breach even where they allege that (1) their data was improperly accessed and (2) their legally protected interest was invaded. The law demands no further proof at

the pleading stage from a plaintiff who has established an actual, concrete invasion of their interests. Speculation as to the future consequences need not be considered at this stage, nor is it appropriate for the court to consider how "burdensome" potential liability might be to future defendants. Mem. Op. 19.

The doctrine of standing "gives meaning to [the] constitutional limits" imposed by the Article III, which "limits the jurisdiction of federal courts to 'Cases' and 'Controversies.'" *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). This doctrine is "built on separation-of-powers principles" and requires that a plaintiff show an "injury in fact" to ensure that she "has a 'personal stake in the outcome of the controversy.'" *Id*. An injury-in-fact is "an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). Where a plaintiff sues to prevent a future injury, an allegation "may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony*, 134 S. Ct. at 2341.

In data breach cases, the legal injury is the very fact—undisputed in this and other data breach cases—that third parties stole plaintiffs' sensitive personal information, a violation of their legally protected interest.[2] Whether defendants are liable for the downstream consequences caused by that breach, and how those consequences should be quantified, are simply irrelevant to the standing analysis.

[2] For example, Plaintiffs in *Storm* allege negligence, breach of contract, and violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law.

The risk consumers face today is simply too great for courts to create unnecessary barriers to hold companies accountable for lax security practices. This Court could not have known when it issued its decision in *Reilly* that data breaches and identity theft would be one of the leading sources of harm to American consumers within five years. But the problem can no longer be ignored, and companies that collect personal information must be accountable if they fail to adopt reasonable data protection measures.

I. Data breaches expose American consumers to unprecedented threats of identity theft and fraud.

A. Americans have suffered an epidemic of data breaches since the *Reilly* decision.

Since this Court decided *Reilly* in 2011, there have been nearly 2,900 publically reported data breaches[3] in the United States. Identity Theft Res. Ctr., *2016 Data Breach Stats* 9 (Apr. 12, 2016)[4] (detailing 247 breaches in 2016 as of April 12); Identity Theft Res. Ctr., *ITRC Breach Statistics 2005 – 2015*, at 1 (2016)[5] (detailing 471 breaches in 2012, 614 in 2013, 783 in 2014, and 781 in 2015). In 2015 alone there were 781 breaches, of which 38% were caused by hacking, 15% by employee error or negligence, 14% by accidental email or

[3] A data breach is "as an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure." Identity Theft Resource Center, *Data Breaches*, http://www.idtheftcenter.org/id-theft/data-breaches.html (last visited Apr. 12, 2016).
[4] http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReport2016.pdf.
[5] http://www.idtheftcenter.org/images/breach/2005to2015multiyear.pdf (last visited Apr. 12, 2016).

internet exposure, 11% by insider theft, and 11% by physical theft. Identity Theft Res. Ctr., *2015 Data Breaches*.[6] Data breaches since 2014 have exposed at least 266 million records containing personally identifiable information. *2016 Data Breach Stats*, *supra* (at least 11,270,651 records exposed in 2016 as of April 12); Identity Theft Res. Ctr., *Data Breach Reports* 4 (Dec. 31, 2015)[7] [hereinafter ITRC 2015 Report] (at least 169,068,506 records exposed in 2015); Identity Theft Res. Ctr., *Data Breach Reports* 4 (Dec. 31, 2014)[8] [hereinafter ITRC 2014 Report] (at least 85,611,528 records exposed in 2014).

Data breaches are so dangerous that the U.S. Director of National Intelligence has repeatedly ranked cybercrime as a top global threat. *E.g.*, *Worldwide Threat Assessment of the US Intelligence Community: Hearing Before the Senate Armed Services Committee*, 114th Cong. 1 (2016) (statement of James R. Clapper, Director of National Intelligence).[9] According to the most recent report by the Department of Justice, more than seventeen million Americans were the victims of identity theft in 2014. *See* Erika Harrell, Ph.D., Bureau of Justice Statistics, *Victims of Identity Theft, 2014*, at 1 (Sept. 2015) [hereinafter *Victims of Identity Theft 2014*].[10] That year, identity theft cost American consumers more than

[6] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html (last visited Apr. 12, 2016). An additional nine percent were caused by a subcontrator or third party, and 7.3 percent by data on the move. *Id.*
[7] http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.
[8] http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf.
[9] http://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.
[10] http://www.bjs.gov/content/pub/pdf/vit14.pdf.

fifteen billion dollars. *Id*. at 7 (outpacing fourteen billion in losses from burglary, automobile theft, and theft). In 2015, the Federal Trade Commission ("FTC") received nearly half a million identity theft complaints from American consumers, a 47% increase from 2014. *See* FTC, *Consumer Sentinel Network Data Book* 5 (Feb. 2016).[11]

Some of the most serious data breaches of the past five years include:

- ***T-Mobile/Experian (2015)***. In October 2015, T-Mobile announced a breach of data housed on an Experian server. T-Mobile, *Frequently Asked Questions About the Experian Incident* (Oct. 8, 2015);[12] *see* ITRC 2015 Report, *supra*, at 45. The hackers stole names, addresses, SSNs, birthdates, identification numbers (e.g., driver's license, military ID, or passport number), and other information for 15 million customers. T-Mobile, *supra*; ITRC 2015 Report, *supra*, at 45.
- ***Excellus BlueCross BlueShield / Lifetime Healthcare (2015)***. In September 2015, a health insurer announced that an attack had exposed names, birthdates, SSNs, mailing addresses, telephone numbers, member ID numbers, financial account information, and claim information. Excellus, *Notice Of Cyberattack Affecting Excellus Bluecross Blueshield* (2015);[13] ITRC 2015 Report, *supra*, at 52–53.

[11] https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf.
[12] https://www.t-mobile.com/landing/experian-data-breach-faq.html.
[13] http://www.excellusfacts.com/.

- ***Ashley Madison (2015)***. In July 2015, hackers stole billing records and account information from an adult social network catering to unfaithful spouses. Brian Krebs, *Online Cheating Site AshleyMadison Hacked*, Krebs on Security (July 19, 2015);[14] *see* Verge Staff, *The Ashley Madison Hack: Everything You Need To Know*, Verge (Aug. 31, 2015).[15] The hackers later made these private details publicly available, exposing the names, relationship status, address, phone numbers, birthdates, and personal attributes of some 36 million users, along with 9.6 million billing records from the users who paid to keep their accounts private. Ross Miller & Frank Bi, *Here's Every Type of Data Exposed in the Ashley Madison Hack*, Verge (Aug. 19, 2015).[16]
- ***Office of Personnel Management (2015)***. In June 2015, the U.S. Office of Personnel Management ("OPM") announced that it had suffered two attacks. Office of Pers. Mgmt., *Cybersecurity Resource Center*;[17] *see* ITRC 2015 Report, *supra*, at 91, 98–99. One attack resulted in the theft of background investigation reports for current, former, and prospective federal government employees, including the SSNs of 21.5 million individuals and 5.6 million fingerprints. OPM, *supra*; ITRC 2015 Report, *supra*, at 91. Earlier that year,

[14] http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/.
[15] http://www.theverge.com/2015/8/19/9178965/ashley-madison-hacked-news-data-names-list.
[16] http://www.theverge.com/2015/8/19/9179037/ashley-madison-data-hack-name-address-phone-birthday/in/8943006.
[17] https://www.opm.gov/cybersecurity/cybersecurity-incidents/ (last visited Apr. 12, 2016).

attackers stole the personnel data of 4.2 million current and former federal government employees, including full names, birth dates, home addresses, and SSNs. OPM, *supra*; ITRC 2015 Report, *supra*, at 98–99.

- ***Premera BlueCross (2015)***. In March 2015, health insurance provider Premera announced that hackers gained accessed to names, birthdates, addresses, telephone numbers, SSNs, member ID numbers, bank account information, and claim information of 11 million customers. Premera BlueCross, *About the Cyberattack* (2016);[18] ITRC 2015 Report, *supra*, at 136–37. The hackers also gained access to private health information. Premera, *supra*.
- ***Anthem (2015)***. In February 2015, health insurance giant Anthem announced that a breach exposed the names, birthdates, SSNs, health care ID numbers, home addresses, email addresses, and employment information for 78.8 million people. ITRC 2015 Report, *supra*, at 152; Anthem, *How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services* (Aug. 25, 2015).[19]
- ***JPMorgan Chase (2014)***. In October 2014, JPMorgan Chase disclosed that a breach had "compromised the accounts of 76 million households and seven million small businesses," gaining names, addresses, phone numbers, and emails. Jessica Silver-Greenberg, Matthew Goldstein, & Nicole Perlroth,

[18] https://www.premera.com/wa/visitor/about-the-cyberattack/.
[19] https://www.anthemfacts.com/.

JPMorgan Chase Hacking Affects 76 Million Households, N.Y. Times (Oct. 2, 2014).[20] Federal authorities ultimately indicted four men for the hack, along with attacks on other financial institutions that disclosed the personal information of more than 100 million individuals. Kim Zetter, *Four Indicted in Massive JP Morgan Chase Hack*, Wired (Nov. 10, 2015).[21]

- ***Home Depot (2014)***. In September 2014, Home Depot announced that a five-month attack on its payment terminals compromised 56 million credit and debit cards and 53 million email addresses. ITRC 2014 Report, *supra*, at 57; Home Depot, *The Home Depot Reports Findings in Payment Data Breach Investigation* 1 (Nov. 6, 2014);[22] Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, Wall. St. J. (Sept. 18, 2014).[23]
- ***eBay (2014)***. In May 2014, eBay announced that a breach had compromised a database containing names, encrypted passwords, email addresses, physical addresses, phone numbers, and birthdates for its 145 million users. ITRC 2014 Report, *supra*, at 103; eBay, *eBay Inc. to Ask eBay Users to Change Passwords* (May 21, 2014).[24]

[20] http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.
[21] http://www.wired.com/2015/11/four-indicted-in-massive-jp-morgan-chase-hack/.
[22] https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf.
[23] http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.
[24] https://investors.ebayinc.com/releasedetail.cfm?releaseid=849396.

- ***Target (2013)***. In November 2013, cybercriminals installed malware on Target's security and payment systems "designed to steal every credit card used at the company's 1,797 U.S. stores." Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg (Mar. 17, 2014).[25] The hackers stole 40 million credit and debit card numbers, and personal information (names, addresses, phone numbers, and email addresses) of 70 million customers. Maggie McGrath, *Target Data Breach Spilled Info On As Many As 70 Million Customers*, Forbes (Jan. 10, 2014).[26]

B. The most severe data breaches involve the disclosure of Social Security Numbers and financial information, which creates a serious risk of fraud and identity theft.

Not all data breaches are created equal. Some breaches are the result of highly sophisticated attacks carried out by anonymous hackers, while others involve physical theft of computers or storage devices containing sensitive records. In some cases the data breached includes highly sensitive information—like SSNs and financial accounts—but other cases involve more generic data that might only be revealing in a specific context. The severity of a data breach will depend on these and other factors. *See* Memorandum for the Heads of Executive Departments

[25] http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.
[26] http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#40c74dec6bd1.

and Agencies from Clay Johnson III, Deputy Director of Management, Office of Mgmt. & Budget, M-07-16, at 14–15 (May 22, 2007) [hereinafter OMB Memo].[27]

Data breaches typically fall into one of three categories: (1) physical theft or misappropriation of devices that contain sensitive data; (2) unauthorized access by an employee or contractor; and (3) intrusion by a remote, and likely unknown, hacker. In each of those categories, the degree of intentionality and level of exposure of the data can vary significantly. A review of recent data breaches cataloged by the Privacy Rights Clearinghouse provides several useful examples of these different types. *See* Privacy Rights Clearinghouse, *Chronology of Data Breaches* (2016).[28]

One of the most severe types of breaches occurs when a hacker remotely downloads sensitive files, as opposed to other more limited or temporary exposure of sensitive information. When malicious hackers gain remote access to SSNs, it poses a grave threat to the victims whose data is compromised. For example, a Maryland contractor recently notified its employees of a breach of their payroll data. *See* Submitted Breach Notification Sample, The Whiting-Turner Contracting Company (Mar. 8, 2016).[29] This breach resulted in the exposure of the name, date of birth, and SSNs of employees and their children. *Id*. The company also received reports that fraudulent taxes were filed in employees' names. *Id*. As in most cases

[27] https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.
[28] https://www.privacyrights.org/data-breach.
[29] http://oag.ca.gov/system/files/Whiting%20Turner%20Contracting%20NOTICE%20only%20CA%20Regulator%20Notice%20Exhibits_0_1.pdf.

where malicious hackers are able to gain access to sensitive personal information, the employees are now at serious risk of identity theft and fraud.

The Office of Management and Budget ("OMB") has identified five factors that should be considered when assessing the severity of a data breach: (1) the nature of the data breached; (2) the number of individuals affected; (3) the likelihood that the information is "accessible and usable"; (4) the likelihood that the breach may lead to harm (both how broad the scope of the harm and how likely it is to occur); and (5) the ability to mitigate the risk of harm. *See* OMB Memo, *supra*, at 14–15.

There is little doubt that when a hacker infiltrates a system containing SSNs and other sensitive personal information, their intent is to access and misuse that data. The black markets where financial and identity information are sold to the highest bidder are "growing in size and complexity," and are now dominated by "financially driven, highly organized, and sophisticated groups," as a comprehensive study by The RAND Corporation recently uncovered. Lillian Ablon, Martin C. Libicki, & Andrea A. Golayix, RAND Corp., *Markets for Cybercrime Tools and Stolen Data,* at ix (2014).[30] These black markets "can be more profitable than the illegal drug trade" and are increasingly resilient even to repeated takedowns by law enforcement. *Id*. at 11, 17. While credit cards, bank accounts, and other payment credentials are the most common type of data stolen

[30] https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

by financially motivated hackers, personal data is also primarily stolen for financial gain. *See* Verizon, *2013 Data Breach Investigations Report* 46 (2013).[31]

A hacker who steals such data can profit in a way that is undetectable to the victim. The dossiers of personal data that can be used to commit fraud—including name, address, and SSN in combination with financial data—are referred to as "Fullz" and can be sold in bulk for as much as $15 per victim. Dell SecureWorks, *Underground Hacker Markets* 14 (2016).[32] Once the data breach occurs, the damage is already done and there is nothing the victim can do to reclaim their personal information.

C. Identity theft causes especially pernicious and long-lasting harm to consumers, far beyond the costs of simple credit card fraud.

Identity theft is not limited to fraudulent credit card charges. When a criminal gains access to an individual's SSN, they can obtain tax refunds and government benefits, receive medical goods and services, apply for employment, and even commit crimes in the victim's name. *See* Identity Theft Res. Ctr., *Identity Theft: The Aftermath* 13 (2014).[33] To make matters worse, a stolen SSN, unlike a stolen credit card, cannot be effectively cancelled or replaced.

The U.S. Government Accountability Office has recognized that "the loss of PII contributes to identity theft," but that "it might take a long time" for the harms

[31] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.
[32] https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report.
[33] http://www.idtheftcenter.org/images/surveys_studies/Aftermath2014FINAL.pdf.

to manifest or be uncovered by the victim. U.S. Gov't Accountability Office, GAO-14-34, *Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent* 11 (2013).[34] Past victims have "lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft." *Id*. Yet these harms do not appear on the victim's bank statement or credit report, and they are nearly impossible to control because of the role the SSN plays as a government and private-sector identifier.

1. SSNs are key to identity theft, but are virtually impossible to replace

The plaintiffs in this case face acute risk because their SSNs and other identifying information were breached. SSNs are the key to our financial, government, and private sector records systems. No other form of identification plays a more significant role in record-linkage, or poses a greater risk to personal privacy. *See* EPIC, *Social Security Numbers* (2016).[35] The SSN is used as both an identifier and an authenticator. *Id*. Put another way, the SSN is both the username and password for an individual's identity. *Id*.

Criminals in possession of SSNs can open new financial accounts and perpetrate identity theft because many financial institutions rely on SSNs to verify transactions. *See* Brian Krebs, *In Wake of Confirmed Breach at Home Depot, Banks See Spike in PIN Debit Card Fraud*, Krebs on Security (Sept. 8, 2014).[36]

---

[34] http://www.gao.gov/assets/660/659572.pdf.
[35] https://www.epic.org/privacy/ssn/.
[36] http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/.

The FTC has recognized that SSNs are the "keys to the kingdom" for identity thieves and that the resulting harm to consumers and businesses is a "major problem in this country, with victims numbering in the millions each year" and losses "in the billions." FTC, *Security in Numbers: SSNs and ID Theft* 2 (Dec. 2008).[37]

The Bureau of Justice Statistics found that "[v]ictims experiencing the opening of a new account or the misuse of personal information had greater [out-of-pocket] loss than those experiencing misuse of an existing credit card or bank account." *See Victims of Identity Theft 2014*, *supra*, at 7. These identity theft victims are also more likely to have unresolved problems more than a year later. *Id*. at 13.

A breach of an individual's SSN causes permanent and irreparable damage to the security of that person's identity, but it is extremely difficult to obtain a replacement number. While the Social Security Administration ("SSA") can issue replacement SSNs, it does so only in limited circumstances, such as "harassment, abuse, or life endangerment." Soc. Sec. Admin., *Can I Change My Social Security Number?* (Mar 11, 2016).[38] Identity theft victims must reach this desperate state before the agency might consider issuing a replacement. The SSA assigns new numbers only if "you've done all you can to fix the problems resulting from

[37] https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf.
[38] https://faq.ssa.gov/link/portal/34011/34019/Article/3789/Can-I-change-my-Social-Security-number.

misuse of your SSN, and someone is still using your number." Soc. Sec. Admin., *Identity Theft and Your Social Security Number* 6 (Feb. 2016) [hereinafter ID Theft and Your SSN].[39] In 2014, the SSA replaced only 250 SSNs due to identity theft misuse. Aarti Shahani, *Theft of Social Security Numbers Is Broader Than You Might Think*, NPR (June 15, 2015).[40]

Even if an identity theft victim has suffered such grievous harm to merit a replacement SSN, problems will continue. The SSA has acknowledged the inadequacy of replacement SSNs, stating that a "new number probably won't solve" your problems because "other governmental agencies" and businesses have records tied to the old number, and "credit reporting agencies will [still] use the number to identify your credit record." *ID Theft and Your SSN*, *supra*, at 7.

2. Identity theft involves much more than fraudulent charges

Many of the problems caused by identity theft are much more difficult to prevent and resolve than fraudulent credit card or bank charges. Criminals can use stolen personal information to commit medical, tax, and other government benefit fraud, to seek employment, and during the commission of other crimes. The consequences for the victims can be dire.

a. Medical Identity Theft

Medical identity theft occurs when a victim's name is used to fraudulently obtain medical goods and services. Stolen patient data, often the target in health

[39] https://www.ssa.gov/pubs/EN-05-10064.pdf.
[40] http://www.npr.org/sections/alltechconsidered/2015/06/15/414618292/theft-of-social-security-numbers-is-broader-than-you-might-think.

care breaches, is "worth 10 times more than your credit card number on the black market." *See* Caroline Humer & Jim Finkle, *Your Medical Record Is Worth More to Hackers Than Your Credit Card*, Reuters (Sept. 24, 2014).[41] This data includes names, dates of birth, insurance policy numbers, and billing information, and is used to file false insurance claims and purchase medical supplies and drugs for resale. *Id*. This type of identity theft is often undetected for years, making "medical data more valuable than credit cards, which tend to be quickly canceled by banks once fraud is detected." *Id*.

Medical identity theft is particularly costly for consumers. According to a recent study, 65% of medical identity theft victims had to spend on average $13,500 and 200 hours to resolve the incident. *See* Ponemon Inst., *Fifth Annual Study on Medical Identity Theft* 1, 2 (Feb. 2015).[42] An estimated 2.32 million Americans have been victims of medical identity theft, with nearly 500,000 new cases in 2014 alone. *Id*. at 8.

The non-economic risks of medical identity theft are also alarming. If the fraudster's medical information is incorporated into the victim's records, that person could receive incorrect diagnoses and treatments. *See* Laura Shin, *Why Medical Identity Theft Is Rising and How to Protect Yourself*, Forbes (May 29,

[41] http://www.reuters.com/article/us-cybersecurity-hospitals-iudUSKCN0HJ21I20140924.
[42] http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

2015)[43] (noting the risk that a victim "could receive medication to which she is allergic, or her record may contain the incorrect blood type").

b. Tax Return, Government Benefits, and Employment Identity Theft Fraud

Stolen SSNs and other personal information are also used to file false tax returns; receive unemployment, food stamps, and Social Security benefits; apply for student loans; and obtain drivers' licenses and passports. *See* FTC, *Guide for Assisting Identity Theft Victims* 43–45 (Sept. 2013) [hereinafter FTC, *ID Theft Guide*].[44] Tax refund identity theft occurs when a criminal uses "an individual's SSN, date of birth, or other PII" to "file a fraudulent tax return seeking a refund." U.S. Gov't Accountability Office, GAO-16-589T, *IRS Needs to Further Improve Controls Over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud* 1–2 (2016).[45] The Internal Revenue Service ("IRS") estimates that it paid out $3.1 billion in fraudulent tax refunds for the 2014 filing season. *Id*.

Employment identity theft occurs when a victim's name and SSN is used to obtain employment. Criminals may user another person's identifying information when applying for jobs if they have a criminal record that may prevent hiring, or if they are not legally authorized to work in the United States. *See* FTC, *ID Theft Guide*, *supra*.

---

[43] http://www.forbes.com/sites/laurashin/2015/05/29/why-medical-identity-theft-is-rising-and-how-to-protect-yourself/#4dead9fde200.
[44] https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.
[45] http://www.gao.gov/assets/680/676493.pdf.

c. *Criminal Identity Theft*

Criminal identity theft occurs when a victim's identifying information is given to law enforcement during the investigation of a crime or upon arrest. *See* FTC, *ID Theft Guide*, *supra*. Victims may be unaware of this fraudulent activity until "the victim is unexpectedly detained, arrested, denied employment, or terminated from employment." *Id*. This type of fraud can occur in crimes from traffic violations to felonies. *See* Aaron Sankin, *How to Change Your Social Security Number If You Get Hacked*, Daily Dot (June 17, 2015).[46]

3. Credit monitoring cannot effectively protect data breach victims from non-financial identity theft.

Credit monitoring provides only weak, short-term assistance to individuals at risk of identity theft, and does not prevent thieves from accessing credit files or opening new accounts. Credit monitoring services only notify victims after fraudulent activity occurs. *See* Brian Krebs, *OPM (Mis)Spends $133M on Credit Monitoring*, Krebs on Security (Sept. 15, 2015).[47] Moreover, companies typically offer credit monitoring for only a year or two after a data breach, but the risk of identity theft can last a lifetime. *See* Identity Theft Res. Ctr., *The Limits of ID-Theft Protection and Credit Monitoring* (Aug. 10, 2015)[48] ("Regardless of how long you may be provided free identity-theft protection as a result of a data breach event, your information can still be misused for eternity."). Certain services do not even

[46] http://www.dailydot.com/politics/change-social-security-number-ssn/.
[47] http://krebsonsecurity.com/2015/09/opm-misspends-133m-on-credit-monitoring/.
[48] http://www.idtheftcenter.org/Identity-Theft/the-limits-of-id-theft-protection-and-credit-monitoring.html.

monitor credit reports at all three major national credit bureaus, creating the potential that consumers may still be left unaware of fraudulent account activity under their names.

Credit freezes, which are sometimes offered after data breaches, can provide some protection against financial fraud, but they can also have severe side effects. Neither a credit freeze nor credit monitoring can be effective at stopping identity theft that does not involve pulling a credit report. *See* FTC, *ID Theft Guide*, *supra*. Credit reports are not involved in cases of medical, tax, and criminal identity theft. Additionally, credit freezes must be lifted whenever an individual needs to run a credit check. "That can create hassles, delays, and other problems if you need to apply for a loan, credit card, or a job; obtain insurance; rent an apartment; set up electric or phone service; and more." Anthony Giorgianni, *Should You Freeze Your Credit File?*, Consumer Reports (Feb. 22, 2014).[49] Many employers will not hire applicants without a credit check. Creating and lifting credit freezes can cost between two to fifteen dollars per bureau. *Id*.

D. Companies need to take adequate precautions in order to avoid data breaches.

The threat of data breach and identity theft may be pervasive, but it is not unavoidable. Many of the most serious breaches that have occurred since *Reilly* could have been avoided by implementing well known data security procedures or minimizing the collection and storage of personal information. Prior investigations

[49] http://www.consumerreports.org/cro/news/2014/02/should-you-put-a-security-freeze-on-the-credit-file/index.htm.

have shown that upwards of 75% of data breaches are possible without any specialized hacking knowledge or skills. Verizon, *2013 Data Breach Investigations Report* 48–49 (2013).[50] In many cases, attackers gain access because of well-known vulnerabilities or carelessness by the company that collected the data.

Many of the most severe breaches were predicted long before they occurred. The OPM Inspector General had "reported critical weaknesses in OPM's ability to manage its IT environment," and "warned that the agency" for years that it "was at an increased risk of a data breach." Office of Pers. Mgmt., Office of the Inspector Gen., 4A-CI-00-15-011, *Final Audit Report: Federal Information Security Modernization Act Audit FY 2015*, at 5 (Nov. 10, 2015).[51]

Many breaches are also made worse by lax security within a company's internal network. An expert report conducted after a 2013 breach revealed that "[o]nce inside Target's network, there was nothing to stop attackers from gaining direct and complete access to every single cash register in every Target store." Brian Krebs, *Inside Target Corp., Days After 2013 Breach*, Krebs on Security (Sept. 21, 2015).[52] Target also failed to respond to security alerts flagging the attack in process. Riley et al., *supra*.

Security experts and courts can agree on baseline principles of reasonable data security. *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 256 (3d Cir.

---

[50] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.
[51] https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf.
[52] http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/.

2015) (finding that the FTC could bring a claim for inadequate data security based on a company's failure to implement several widely accepted data security practices); *Cybsersecurity and Data Protection in the Financial Sector: Hearing Before the Subcomm. on Fin. Inst. & Consumer Credit of the H. Comm. on Fin. Servs.*, 112th Cong. 12 (Sept. 14, 2011) (testimony of Marc Rotenberg, Executive Director, EPIC)[53] (noting that companies "need to know that they will be expected to protect the data they collect and that, when they fail to do so, there will be consequences").

An expert panel chaired by Willis Ware explained in 1970 that a "combination of hardware, software, communication, physical personnel, and administrative-procedural safeguards is required for comprehensive security." Def. Sci. Bd. Task Force on Comput. Sec., *Security Controls for Computer Systems*, at vi (1970).[54] Companies that collect and store consumer information must develop a proactive and comprehensive security plan, tailored to the organization's business objectives and information systems. IBM, *Winning the Battle of the Breach* (2015).[55] The plan should address data minimization, IT systems, and organizational procedures. *See generally* Kroll, *Data Breach Prevention Tips* (2015);[56] Symantec, *6 Steps to Prevent a Data Breach* (Nov. 2009).[57]

---

[53] http://financialservices.house.gov/uploadedfiles/091411rotenberg.pdf.
[54] https://assets.documentcloud.org/documents/2800105/Document-01-Defense-Science-Board-Task-Force-on.pdf.
[55] https://www-03.ibm.com/security/data-breach/prevention.html.
[56] http://www.kroll.com/en-us/cyber-security/data-breach-prevention/cyber-risk-assessments/data-breach-prevention-tips.

First, companies should embrace data minimization; criminals can't steal what a company doesn't have. White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy* 21 (Feb. 23, 2012)[58] (stating that companies "should collect only as much personal data as they need to accomplish purposes" and "should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise"); Kroll, *supra*. Companies should only collect information as needed and purge it once the need is gone, should limit the number of places where data is stored, and should grant employees access to data only on an "as-needed" basis. *Consumer Data Protection in a Networked World*, *supra*; Kroll, *supra*; *see also* Ernie Hayden, *Data Breach Protection Requires New Barriers*, SearchSecurity (May 2013)[59] (discussing "islanding" sensitive data to minimize breaches).

Second, if companies do choose to collect and store consumer data, they must implement adequate technical protections. Industry standards now provide a comprehensive framework to guide companies that handle sensitive consumer data. Brief for EPIC and Thirty-Three Technical Experts and Legal Scholars as Amicus Curiae Supporting Respondents, FTC v. Wyndham Worldwide Corp., 799

---

[57] http://eval.symantec.com/mktginfo/enterprise/other_resources/b-6-steps-prevent-data-reach_20049431-1.en-us.pdf.
[58] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[59] http://searchsecurity.techtarget.com/feature/Data-breach-protection-requires-new-barriers.

F.3d 236 (3d Cir. 2015) (No. 14-3514)[60] (outlining three well-established cybersecurity standards that detail how database operators must identify vulnerable hardware, protect sensitive data, and respond to attacks). Last year, this Court found that Wyndham had fair notice of its inadequate cybersecurity practices when it stored payment card information in clear readable text, allowed easily guessed passwords, failed to use readily available security measures (such as firewalls, IP address restrictions, and encryption), failed to adequately restrict the access of third-party vendors to its networks, failed to employ reasonable measures to detect and prevent unauthorized access, and failed to follow proper incident response procedures. *Wyndham*, 788 F.3d at 240–41, 256.

Finally, companies must strengthen organizational procedures that build and reinforce a culture of security. Kroll, *supra*. Companies must educate employees "about appropriate handling and protection of sensitive data." *Id.*; *see also* IBM, *supra*. To prevent inadvertent (or intentional) breaches, they must also develop protocols for remote access, on- and off-site data storage, and employee exit. Kroll, *supra*. Companies should ensure that venders and partners maintain the same data security standards to prevent indirect attacks. *Id.*

Data breaches are one of the largest threats facing American consumers today. Reasonable data security measures can help to minimize the risk of attack and reduce the consequential harm if a breach occurs. Courts should ensure that the law encourages improved data security standards. Creating barriers to those who

[60] https://epic.org/amicus/ftc/wyndham/Wyndham-Amicus-EPIC.pdf.

seek to strengthen data protection will magnify the risks American consumers already face.

II. Companies that collect and store sensitive consumer data are in the best position to prevent data breaches, and should be held liable when they fail to adopt reasonable data security measures.

The lower court fundamentally misunderstood the role of liability in preventing accidents when it lamented that data breach suits would be "unduly burdensome" to business. Mem. Op. 19. Liability for data breaches is necessarily assigned to companies in order to internalize the harms that follow from the company's decisions to (a) collect and use personal information but (b) not adopt reasonable data security measures. Without the appropriate allocation of liability, there is little reason for a company to invest in prevention and mitigation. Even worse, misallocation of liability allows companies to profit from consumers' personal information but leave them to bear the immediate harms and downstream consequences of the company's failure to implement data security.

The doctrine of reasonable care is based on the theory that the party who is in the best position to avoid harm—i.e., the "least-cost avoider"—should bear the costs of an accident. *See* Guido Calabresi, *The Costs of Accidents: A Legal And Economic Analysis* 135 (1970) ("A pure market approach to primary accident cost avoidance would require allocation of accident costs to those acts or activities (or combinations of them) which could avoid the accident costs most cheaply."); *see also* Richard Coase, *The Problem of Social Cost*, 3 J. Law & Econ. 1 (1960) (articulating a theory of cost allocation to promote efficient allocations of property resources). Liability rules that hold a least-cost avoider responsible for

unreasonable conduct thus create the socially efficient outcome of least consequential harm at least preventative cost.

Correctly identifying the least-cost avoider becomes particularly important where transaction costs are high, as in the case of one party injuring a large and diffuse group of individuals. Calabresi, *supra*, at 135–38; *see* Harold Demsetz, *When Does the Rule of Liability Matter?*, 1 J. Legal. Stud. 13, 27–28 (1972) (arguing that when transaction costs are high, the legal system can "improve the allocation of resources by placing liability on that party who in the usual situation could be expected to avoid the costly interaction most cheaply").

"Database operators"—such as companies that collect and store consumer data—"constitute the cheapest cost avoiders vis-à-vis individuals whose information sits in a private entity's database." Danielle Keats Citron, *Reservoirs of Danger: the Evolution of Public and Private Law at the Dawn of the Information Age*, 80 Southern Cal. L. Rev. 241, 284 (2007) (arguing that data brokers should be strictly liable for unsecure databases and data breaches); *cf.* Brief for EPIC as Amicus Curiae Supporting Appellants, at 3–4, Gordon v. Softech Intern., Inc., 726 F.3d 42 (2d Cir. 2013) (No. 12-661) (arguing for similar liability for resellers of driver's records). A company maintaining databases of consumer data "has exclusive knowledge about, and control over, its information system." Citron, *supra*, at 285. Critical for effective minimization of threats, these companies "have distinct informational advantages about the vulnerabilities in their computer networks." *Id.*

Consumers do not have the ability to avoid these breaches because they "have no information about, and have no practical means to find out, where their personal data resides" or how it is protected. *Id.* at 285–86; *see also Understanding Consumer Attitudes About Privacy: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the House Comm. on Energy and Commerce* 102–03 (Oct. 13, 2011) (testimony of Prof. Alessandro Acquisti)[61] ("Research has suggested that US consumers are often ill-informed about the collection and usage of their personal information, and the consequences of those usages. This puts them in a position of asymmetric information, and sometimes disadvantage, relative to the data holders that collect and use that information.").

Even if consumers knew where to look, they "cannot detect and understand the security offered" by database operators. Citron, *supra*, at 284–85. "Even individuals knowledgeable about information security will find it difficult to assess how well a database system is designed and implemented." *Id.* at 285. And even if consumers did know how to secure their data, "it is unclear what [they] could do if informed about a database operator's vulnerabilities." *Id.*

Unlike the companies, consumers cannot effectively insure against the risk of identity theft. *Id.* Experts have found that identity theft insurance "falls way short" of what consumers need. Priya Anand, *Is Identity-Theft Insurance a Waste*

[61] https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg74605/pdf/CHRG-112hhrg74605.pdf.

of Money? MarketWatch (Mar. 31, 2014).[62] Unlike car insurance, which covers car damage and personal injuries, identity theft insurance doesn't cover the injuries consumers suffer after their identity is stolen. Nancy Mann Jackson, *Identity Theft Insurance: How Does It Work and Will It Save Your Good Name?*, Bankrate (June 15, 2015).[63] These policies reimburse for certain enumerated costs: phone bills, notary and certified mailing costs, lost wages, or attorney fees. *Id.* But they do not reduce the most substantial cost: "the time and hassle required to rectify the situation." *Id.*

The data breach problem also cannot be solved through simple market economics. Citron, *supra*, at 286. Bringing together hundreds of millions of consumers to bargain with every database operator would be prohibitively expensive and logistically impossible. *Id.* "Large consumer blocks also encounter difficulty expressing collectively their relative preferences." *Id.* (internal quotation marks and modifications omitted). These substantial transaction costs counsel towards "imposing liability on the party best able to reduce costs" in order to result "in the most efficient allocation of resources." *Id.* at 286–87 (citing Demsetz, *supra*).

Consequentially, the company collecting and storing consumer data "sits in the best position to make decisions about the costs and benefits of its information-gathering" and distribution. *Id.* at 285. As such, they must bear the cost for failing

[62] http://www.marketwatch.com/story/is-identity-theft-insurance-a-waste-of-money-2014-03-31.
[63] http://www.bankrate.com/finance/insurance/insurance-identity-theft-1.aspx.

to implement adequate data security. But correct allocation of responsibilities does not by itself result in the efficient minimization of harm. If defendants liable for legal injury do not actually implement adequate data security measures, then consumers will continue to be injured and face devastating downstream harms.

Non-litigation methods are currently insufficient to incentivize companies to implement reasonable data security protections. No federal agency has sufficient authority to issue or enforce rules establishing minimum data security standards. The only federal agency that has been active in enforcing data security standards against commercial data collectors is the FTC, which can only do so under its "unfair or deceptive" trade practices authority. *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015) (holding that the FTC can regulate cybersecurity as an unfair trade practice). The only recent proposal considered by Congress, a federal data breach notification rule, would not address security standards. *See* White House, *Fact Sheet: Safeguarding American Consumers & Families* (Jan. 12, 2015).[64]

Litigation, therefore, is an important mechanism to ensure that personal data is adequately protected. *See* Richard A. Posner, *Economic Analysis of Law* 491 (3d ed. 1986) (stating that the legal system determines "what allocation of resources would maximize efficiency" when "the costs of a market determination would exceed those of a legal determination"). Damages also force defendants to

[64] https://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

internalize the full measure of the harm and take sufficient care to prevent future injury. *See Friends of the Earth, Inc. v. Laidlaw Envtl. Serv. (TOC), Inc.*, 528 U.S. 693, 185 (2000) (finding that civil penalties have a deterrent effect and can therefore prevent future injury).

What the lower court in this case has failed to recognize is that there are at least four distinct categories of damages caused by data breaches: (1) the costs of mitigating identity theft and financial fraud; (2) the increased risk of identity theft and fraud; (3) unauthorized transactions and credit-based identity theft; and (4) more pernicious forms of identity theft, *see* Part I.C, *supra*. The lower court mistakenly assumed that credit-based fraud is the only category of damages, concluding that the plaintiffs' "credit information and bank accounts look the same today as they did prior to" the data breach. Mem. Op. 14. By excluding recovery for the other three categories of damages, the lower court allowed the defendant to ignore the wide range of risks consumers face because of the company's lax security practices. Victims will be unable to seek redress for the most pernicious costs of data breach, including damage to their reputation, employment prospects, and credit.

Since the *Reilly* decision in 2011, the problem of data breaches has become widespread in the United States. Few dispute the growing risks. To erect barriers to those who now seek to improve data protection invites more identity theft and financial fraud in the future.

CONCLUSION

EPIC respectfully requests that this Court reverse the lower court's order granting Appellee's motion to dismiss.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
Counsel of Record
Alan Butler
Claire Gartland
Aimee Thomson
Electronic Privacy Information Center
1718 Connecticut Ave. N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULES

This brief complies with the type-volume limitation of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 6,853 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word for Mac 2011 in 14 point Times New Roman.

Dated: April 18, 2016

/s/ Marc Rotenberg
Marc Rotenberg

CERTIFICATE OF COMPLIANCE WITH LOCAL RULES

I certify that I have complied with LAR 31.1(c) because this file was scanned by the most current version of Virus Total, https://www.virustotal.com, and no virus was detected. I also certify that I am a member of the bar of this court, and that the text of this electronically filed brief is identical to the text of the 10 paper copies mailed to the court.

Dated: April 18, 2016

/s/ Marc Rotenberg
Marc Rotenberg

CERTIFICATE OF SERVICE

I hereby certify that on April 18, 2016, I electronically filed the foregoing Brief of *Amici Curiae* Electronic Privacy Information Center Support of Appellant with the Clerk of the United States Court of Appeals for the Third Circuit using the CM/ECF system. All parties are to this case will be served via the CM/ECF system.

Dated: April 18, 2016

/s/ Marc Rotenberg
Marc Rotenberg